Computer virus prevention: a primer

Jan Hruska, Sophos Plc, Oxford, England

First published: August 2000

SUMMARY

This white paper describes the current virus situation, common virus entry points, procedures for preventing infection, types of anti-virus software, deployment and administration of anti-virus software, and measures for recovering from a virus attack.

Viruses today

Known viruses surpassed 50,000 in August 2000.

The number of known viruses surpassed 50,000 in August 2000. A large majority of those (74%) are parasitic viruses (attacking executables), second are macro viruses (19%) and 7% are boot sector viruses. In May 2000 88% of infections reported to Sophos were due to macro viruses, 9% due to parasitic viruses and only 3% due to boot sector viruses. Note that a reported infection is counted as a single unit regardless of whether the virus infected one machine or 10,000 machines: the statistics quoted are not 'bomb-proof' but simply an indication of what is out there.

The number of new viruses discovered every month continues to increase. In the second quarter of 2000, the Sophos virus lab was processing 800 new viruses every month.

It is impossible to predict which new virus will be released "in the wild" and cause problems. All have to be analysed and detection/disinfection for them included in anti-virus software.

Anti-virus companies are all faced with the dilemma of how to prioritise detection of viruses reaching their virus laboratory. It is impossible to predict which (if any) of the new viruses will be released 'in the wild' and start causing problems: new viruses must simply be analysed and the detection/disinfection for them included in the anti-virus software. However, there is a group of viruses which have a greater **potential** to spread rapidly. Viruses which are 'internet-enabled' and which exploit some form of common social engineering factor (such as the LoveLetter virus) obviously fall into this category.

Anti-virus procedures

Using anti-virus software should not be the only component of an effective anti-virus defence. What are the other components?

Stop using DOCs

Stop using DOC and XLS file formats. Use RTF and CSV file formats instead.

Use Rich Text Format (RTF) files instead. All the Word text formatting will be saved, but RTF files cannot contain macros and, hence, cannot be used to spread viruses.

Beware, though: a received Word file with an RTF extension is not necessarily a Rich Text Format file. Word can save files in Word format (i.e. with macros) under any extension.

Stop using XLSs

Use CSV format instead. Similar caveats apply as for using RTF files.

Use PowerPoint 7 or earlier

PowerPoint 7 or earlier does not have macro capability and, as such, is inherently virus-proof. Unfortunately, the visual appearance of PowerPoint 8 presentations is much better than PowerPoint 7 and the struggle to convince users that a virus-free environment is preferable to a visually more appealing one is very much an uphill one.

Use viewers, not applications

When the user double-clicks on an attachment, most systems are configured to start the application associated with the file type. For example, a DOC file will start Word, an XLS file Excel etc. The trouble is that these applications will also execute any macros within the received file, thus enabling the virus to infect.

Most email applications can be configured to view a received file using a 'viewer'. Viewers normally do not have macro capabilities. Even if an infected file is examined in such a way, the virus will not infect the environment. Most users do not need to edit the received attachments, which makes using this strategy throughout the organisation a very effective anti-virus technique.

Block receiving/sending of executable code

There is very little need for executable code to be sent. Where ZIP compressed data files are sent, using statically compressed ZIPs (which need PKUNZIP to be decompressed) is better.

There is very little need for executable code to be received or sent. In most instances it is also illegal, usually breaching the software copyright. Some people are fond of using self-extracting ZIP files to send compressed data files: for security reasons using statically compressed ZIPs (which need PKUNZIP to be decompressed) is a much better solution.

The blocking of executable code transfer is often best achieved on the internet gateway. Unfortunately, it is impossible to detect executable code with 100% certainty by analysing either the file content or the file extension. However, blocking files with executable extensions such as EXE, VBS, SHS etc. contributes to overall anti-virus measures.

User education also plays a significant part in preventing infections by executable code received by email: the temptation to install a cute screen saver can be very, very high for a PC user who is not security aware.

Change the CMOS boot-up sequence

Most PCs are configured as delivered from the manufacturers to boot from drive A: first, and only if there is no disk in the drive to boot from drive C:. If a user leaves an infected disk in the floppy drive, the PC will become infected as the result.

Changing the PC to boot from drive C: completely eliminates the danger from pure boot sector viruses.

On modern PCs the booting sequence is stored in the CMOS memory and is very easy to change. Changing the PC to boot from drive C: completely eliminates the danger from pure boot sector viruses. If the PC needs to be booted from the floppy in the future, reversing the boot sequence is easy.

Most organisations, however, do not use this simple technique.

Turn off Windows Scripting Host

Windows Scripting Host should be turned off.

If the Windows Scripting Host (WSH) is not used, it should be turned off. The procedure is described at http://www.sophos.com/support/faqs/wsh.html.

Keep an eye on security bulletins

Up to November 1999, anti-virus experts could state authoritatively that a PC cannot get infected by simply reading email. Of course, they had analysed the current technology specifications and there really was no apparent way of infecting a PC purely by reading email. Unfortunately, there was a difference between the specification for Microsoft Outlook and what the code was actually doing (also known as a programming bug), which allowed the virus BubbleBoy to infect when a user read email. Microsoft issued a patch which corrected the problem (see Microsoft Security Bulletin MS99-032) but very few users implemented it. Kakworm, which exploits the same loophole, is one of the most common viruses today.

Kakworm, which exploits a security loophole, is one of the most common viruses today.

The complexity of today's software required by the never-ending thirst for new features, pretty pictures and sophistication, results in more people writing software to ever tighter deadlines (invariably reducing the average programmer competence level and the software quality). There is little point in complaining that the Windows operating system and the software written for Windows is unreliable: market demand is by far the main culprit for indirectly causing the unreliability.

This situation is not going to get better. The best that an organisation can do is to keep an eye on the various security bulletins which publicise security-related bugs.

Backups

Data destruction is only one of the side-effects found in viruses. It is neither new nor the worst thing that can happen to data. Backups have been a component of computer security from the early days of computers, guarding against the inevitable component failures and the resulting loss of data.

Data corruption is much worse than data destruction. It is often difficult to detect, so it may take months to be noticed.

Data corruption is much worse than data destruction. It is often difficult to detect, which means that it may take months before it is noticed. Resorting to backups to retrieve the data is often not an option, since documents and spreadsheets change and the document retrieved from the backup may be far too old to be of use.

Nevertheless, backups continue to be a necessary part of an effective defence against computer viruses.

Anti-virus software types

Scanners

Scanners are by far the most popular type of anti-virus software used today. They contain detection/disinfection information for all known viruses. They are intuitive to use and capable of identifying a virus (e.g. "ABC.DOC is infected with the 'Blah' virus").

The main disadvantage of scanners is that they need to be kept updated with the latest virus information in order to remain effective.

Checksummers

Checksummers rely on detecting change. When a virus infects an object, the object will change. The change will be picked up by the scanner. Checksummers will pick up both known and unknown viruses, as long as the virus changes an object monitored by the checksummer.

The main difficulty with using checksummers is distinguishing between legitimate and viral change. In other words, the results from checksummer findings need expert interpretation (normally not available at the user level). Another problem is that checksummers will detect a virus only once an infection happens; they cannot be used to prevent an infection. Virus detection alone is clearly undesirable.

Heuristics

Heuristic-based software applies rules to distinguish viruses from non-viruses. Unfortunately, it is not problem-free.

Heuristics (from the Greek heuriskein, to discover, find) is a rule of thumb, strategy, method or trick used to improve the efficiency of a system that tries to discover the solutions to complex problems. In the context of anti-virus software, it is used to describe software which applies rules to distinguish viruses from non-viruses. Heuristic software is initially attractive for users since it is often presented as not needing updates.

Unfortunately, heuristics is not problem-free. The main problem is that the virus writing community learn the rules used by heuristic software very quickly and start writing viruses which circumvent them. The anti-virus companies then reformulate the rules and reissue the software etc., annulling the 'no updates' argument. Heuristic software also has a propensity to 'false alarm', i.e. to label objects as viruses when they are not. It is this problem that makes heuristic software a less likely choice in the corporate environment.

Virus entry points

In order to establish where anti-virus software should be deployed in an organisation, it is important to establish what are the common virus entry points.

Email

An overwhelming proportion of infections today are caused by infected email attachments.

An overwhelmingly large proportion of infections today are caused by infected email attachments. The ease with which a user can click on an attachment and launch an application is a significant factor in the spread of email-borne viruses. If the email content is sufficiently inviting (e.g. "kindly check the attached LOVELETTER coming from me.") and the visible attachment extension sufficiently innocent in the eyes of an average user (e.g. LOVE-LETTER-FOR-YOU.TXT.vbs - text files cannot carry an infection, can they?), the temptation for a user can become overwhelming.

The danger of infection through attachments is, of course, not confined to email. Newsgroup postings are also capable of carrying attachments and the number of new infected attachments currently discovered by automated newsgroup scanners is around 10 per day.

World Wide Web

The web is crawling with sites carrying virus-infected material. Desktop access to the web is not only technologically possible but also viewed as an 'expected' in today's workplace. Downloading potentially infected files is too easy.

Several organisations have found that providing physically separate PCs to access the web is a good arrangement.

Several organisations have, however, found that providing physically separate PCs to access the web is a much better arrangement. Not only is the web physically separated from the company main network, but employees tend to waste much less time 'surfing' non work-related sites, since it is obvious when they are not seated at their desks.

Floppy disks and CDs

The use of floppy disks has decreased radically with the advent of networks, but most PCs still come with a floppy drive fitted as standard. 3% of all infections are due to boot sector viruses, which shows that floppy disks are not dead (yet). CDs (especially magazine cover CDs) have also been shown to be relatively frequent virus carriers.

Anti-virus software deployment points

Anti-virus software should be deployed on internet gateways, servers and desktops.

There are three main points where it makes sense to deploy anti-virus software: on the internet gateway, on the servers and on the desktop.

Internet gateway

The internet gateway is the point that connects the internet and internal company networks. It is a good place to install anti-virus software which will check incoming and outgoing email attachments.

The main advantage of using anti-virus software on the gateway is that infected attachments sent to multiple email addresses will generate a single virus alert (on the gateway) instead of multiple ones if the infected email is allowed to get through to the desktop.

The main disadvantage of using anti-virus software on the gateway is the slower turnover of emails through this bottleneck.

At the moment, relatively few emails are encrypted and the effectiveness of gateway scanning is high. This will decline in the future.

A problem of using anti-virus software on the gateway which is important to bear in mind is the increasing use of encryption. There is no point in checking encrypted attachments since viruses will be safely hidden inside the encryption envelope. At the moment, only relatively small numbers of emails are encrypted and the effectiveness of gateway scanning is still high. This will decline in the future.

Servers

Using anti-virus software on servers to scan centrally held files has several advantages over trying to scan the servers from a workstation. Firstly, network traffic is minimised since the scanning process runs locally on the server. Secondly, any virus stealth mechanisms are not effective since the virus is never 'active' on the server.

Most organisations deploy anti-virus software to scan their servers at regular intervals, usually during periods of low user activity.

Desktop

Virus scanning on the desktop is probably the most important part of the three-point scanning strategy.

Virus scanning on the desktop is probably the most important part of the three-point scanning strategy. Even if the virus penetrates the internet gateway scanner by arriving in an encrypted email, even if it is not caught by the server scanner (which does not scan email), it will have to be caught by the desktop before it is allowed to infect.

It is often the case that keeping desktop anti-virus software up to date is one of the hardest tasks faced by the system administrator. This is especially the case on the desktops not permanently connected such as laptops with docking stations.

Anti-virus software administration

Since the effectiveness of anti-virus software in use today depends on frequent updates, it is very important that effective tools are available to deploy, upgrade and administer anti-virus software throughout the organisation.

Updates over the internet

Updating anti-virus software automatically over the internet is an attractive concept for system administrators. However, it has implications for organisation security as it outsources control to the anti-virus software supplier.

Automatically updating anti-virus software over the internet is an attractive (zero workload) concept for system administrators. It does, however, have deep implications for the overall security of the organisation since it effectively outsources the control and the decision-making process over what software gets installed on the company network to the anti-virus software supplier. Few organisations are happy with this, preferring to place a human specialist in the loop. The specialist can then decide what, how and when to deploy the updates. Any such new software can also be tested before being deployed company-wide.

Administration

The administrator of a large anti-virus software installation needs the tools to communicate with the anti-virus software effectively (admin->software->admin). The software needs to be kept updated (admin->software) while the administrator needs regular feedback, both virus and non-virus related (software->admin).

Three main techniques are used to distribute updates over the company network: push, pull and combined push/pull. Each has its advantages and disadvantages and the decision on which is best suited will depend heavily on the network structure, speed of connections, network usage patterns etc.

Recovery from virus attack

Should a virus manage to penetrate the defences placed in its path, the company must have effective procedures in place to contain the infection on as few PCs as possible.

Should the unthinkable happen and a virus manages to penetrate all the defences put in its path, the company must have effective procedures in place to be able to contain the infection on as few PCs as possible as well as restoring these PCs to their pre-infection state. This is a relatively complex subject with no easy solutions.

Such virus penetration usually occurs when the anti-virus software used does not recognise a particular virus. Cultivating a good relationship with the anti-virus software supplier and knowing that they will jump in an emergency is an important factor in the company's anti-virus strategy.

Dealing with a virus that has been allowed to enter a company will be orders of magnitude more expensive than the cost of any anti-virus software. The main expense will be time, since it will probably be necessary to visit every infected workstation to perform the disinfection and its restoration to the pre-infection state.

Having company-standard software installations, possibly supplemented by disk imaging software, can be very helpful in restoring infected workstations.

SOPHOS

Sophos Plc • The Pentagon • Abingdon • Oxfordshire • OX14 3YP • UK
Tel +44 01235 559933 • Fax +44 01235 559935

www.sophos.com